AN ANALYSIS OF THE NIGERIAN DATA PROTECTION REGULATION 2019

The continuous shift from manual to digital processes across various sectors globally has necessitated the publication of data protection legislation by governments across the world. These legislations seek to regulate the collection, collation, storage and processing of personal data by private, public and government entities as well as safeguarding the information of individuals obtained through digital processes.

As a result of the foregoing, and the lack of data protection laws in Nigeria, there was a clamor by various stakeholders in the country for the development of an efficient data protection regime in Nigeria, in line with global standards. In response to this, the National Information Technology Development Agency ("the NITDA") being the primary body responsible for the administration and monitoring of the use of electronic data and other forms of electronic communication transactions, on the 25th of January, 2019 released the NITDA Data Protection Regulation 2019 ("the Regulation") which replaced the NITDA Guidelines 2017 ("the Guidelines") and remains till date, the most comprehensive generally applicable legislation on data protection in Nigeria.

It is pertinent to point out that the General Data Protection Regulation (GDPR), the legal framework which sets out the guidelines for collection and processing of personal information of individuals in the European Union is the foundational piece of legislation upon which the Regulation was drafted.

The Regulation seeks to capture international best practices regarding:

a) Safeguarding the rights of natural persons to data privacy;
b) Fostering safe conduct of transactions involving the exchange of personal data;
c) Preventing manipulation of personal data;
d) Ensuring that Nigerian businesses remain competitive in international trade through the safeguards afforded by a just and equitable legal regulatory framework on data protection; and
e) Ensuring that the Nigerian Data protection framework is consistent with global best practices.

The Regulation applies to:

a) All transactions which require the processing of personal data irrespective of the means by which the data is processed or intended to be processed in respect of natural persons in Nigeria; and
b) Natural persons residing in Nigeria or residing outside Nigeria but of Nigerian descent.

KEY HIGHLIGHTS OF THE REGULATION

The following are the highlights of the regulation**:**

a) PRIVACY POLICY

The Regulation requires any medium or organisation through which personal data is being collected or processed to display a simple and conspicuous privacy policy that the class of persons whose personal data is to be collected or processed ("Data Subjects") can understand.

The Privacy Policy is required to contain provisions relating to the following:

- what constitutes the Data Subject's consent to the collection and processing of his or her personal information;
- a description of collectable personal information;
- purpose of collection of personal data;
- the technical methods used to collect and store personal information;
- a highlight of the principles of the Regulation;
- the available remedies in the event of violation of the privacy policy;
- the time frame for remedy and any limitation clause.

b) DATA SECURITY

The Regulation places an obligation on anyone or organisation involved in data processing or the control of data to develop security measures to protect such data. Protective measures include but are not limited to protection against hackers, setting up firewalls, storing data securely with access to specific authorized individuals, employing data encryption technologies, developing organizational policy for handling personal data (and other sensitive or confidential data), protection of emailing systems and continuous capacity building for staff.

c) THIRD PARTY DATA PROCESSING CONTRACTS

The Regulation requires that data processing by a third party should be governed by a written contract between the third party and the Data Controller i.e. any person or body that determines the purposes for and the manner in which personal data is processed or is to be processed. Any person or organisation

engaging a third party to process the data obtained from Data Subjects shall ensure strict adherence to the Regulation.

d) DATA PROTECTION COMPLIANCE ORGANISATIONS

The Regulation empowers the NITDA to register and license Data Protection Compliance Organizations (the "DPCOs") who on behalf of NITDA will monitor, audit, conduct training and data protection compliance consulting to all Data Controllers under the Regulation.

e) DATA SUBJECT'S RIGHT OF OBJECTION

The Regulation provides that a Data Subject has the right to object to the processing of his or her data at any time. Consequently, the Data Subject has the right to (i) object to the processing of his personal data by the Data Controller for marketing purposes, and (ii) be expressly and manifestly offered the mechanism for objection to any form of data processing at no cost whatsoever to the Data Subject.

f) TRANSFER TO A FOREIGN COUNTRY

The Regulation stipulates the conditions under which personal data which is being processed or intended for processing can be transferred to a foreign country or to an international organisation. It requires that any such transfer must be carried out under the supervision of the Honorable Attorney General of the Federation (AGF). The AGF is expected to assess the level of protection within the legal system of that foreign country or the international organisation and, if satisfied, confirm that the protection levels in the foreign country or organisation are adequate to protect the Data Subject's personal data.

The Regulation provides exceptions and circumstances under which a transfer may be undertaken without the prior assessment by the AGF. They include:

- where explicit consent of the Data Subject is obtained for the transfer of personal data to a foreign country or an international organisation without adequate affirmation by the AGF, the consequence of the absence of the AGF's decision having been made clear to the Data subject, and that there are no other alternatives to the transfer;
- where the transfer is necessary for the performance of a contract between the Data Subject and the Data Controller or the implementation of pre-contractual measures taken at the Data Subject's request;
- where the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Data Controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defense of legal claims;

- the transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent;

g) ISSUANCE OF DATA PROTECTION POLICIES AND AUDIT

The Regulation prescribes that all public and private organizations in Nigeria that control data of natural persons shall within 3 months after the date of the issuance of the Regulation make available to the general public their respective data protection policies which should conform with the provisions of the Regulation. Every Data Controller has the obligation of designating a Data Protection Officer for the purpose of ensuring adherence to the Regulation and each organisation is required to conduct a detailed audit of its privacy and data protection practices within 6 months of the issuance of the Regulation.

Data Controllers who process the personal data of more than 1000 Data Subjects within a period of six months are required to submit a summary of the audit report to NITDA while Data Controllers who process personal data of more than 2000 Data Subjects within a period of 12 months are required to submit a summary of their data protection audit to NITDA on an annual basis, not later than the 15th of March of the following year.

h) PENALTY FOR DEFAULT

The penalties for a breach of the Regulation are (in addition to any other criminal liability that such breach might give rise to) as follows:

- in the case of a Data Controller dealing with more than 10,000 Data Subjects, payment of the fine of 2% of its annual gross revenue of the preceding year or payment of the sum of N10,000,000.00 (ten million Naira), whichever is greater;
- in the case of a Data Controller dealing with less than 10,000 Data Subjects, payment of the fine of 1% of its annual gross revenue of the preceding year or payment of the sum of N2,000,000.00 (two million Naira), whichever is greater.

AN ANALYSIS OF THE PROVISIONS OF THE REGULATION

SCOPE OF THE REGULATION

In outlining its scope, it is pertinent to note that the Regulation does not contemplate the protection of entities as it specifically refers to only natural persons and not artificial persons in law. The Regulation also intends to apply to "**natural persons residing outside of Nigeria but of Nigerian descent".** While the intentions of the NITDA to protect data of

persons of Nigerian descent regardless of their country of residence is commendable, the enforcement of the Regulation outside Nigeria will pose potential challenges.

In its Section 1, the Regulation provides that it does not operate to deny any Nigerian or any natural person the privacy rights they are entitled to under any law, regulation, policy, and contract for the time being in force in Nigeria or any foreign jurisdiction. As such, the Regulation looks to operate as an added layer of protection to existing data protection legislation locally and internationally.

Furthermore, the Regulation expressly distinguishes between personal data and sensitive personal data in its definitions but other than the distinction in its definitions, there are no varying prescribed standards in the treatment to be accorded to personal data and sensitive personal data and as such the same degree of protection is to be accorded to both.

SECURITY/BREACH OF DATA

The Regulation provides that personal data should be protected against all conceivable hazards and breaches such as theft, cyber-attack, viral attack, dissemination, and manipulation of any kind. It goes ahead to prescribe the means of achieving the protection, by requiring anyone involved in data processing or the control of data to develop security measures which include development of system/mechanisms to prevent hacking, use of firewalls, secure storage of data with restriction of access to specific authorized individuals, use of data encryption technologies, development of organizational policy for handling personal data and other sensitive or confidential data, protection of emailing systems and continuous capacity building for staff.

The Regulation clearly requires data processors and controllers to act with all reasonable diligence to prevent and secure a breach of data which they process or is in their custody as they shall be liable for the actions or inactions of third parties who handle the personal data of data Subjects. As such, they must ensure that the system of any such third party is of the required standard by verifying the integrity of the said system.

ADEQUACY OF SECURITY AND BREACH PREVENTION MEASURES

Upon a casual glance at the provisions of the Regulation, it would seem that the Regulation provides sufficient security measures for protection of personal data as it provides that personal data be protected against every conceivable form of breach and hazard and provides the specific security measures to be taken in furtherance of the required protection. However, upon further consideration of these provisions in

comparison with similar provisions in other African jurisdictions, the insufficiency of these provisions under the Regulations will be revealed.

The South African Protection of Personal Information Act 2013 (PPIA) and the Ghanaian Data Protection Act 2012 (GDPA) requires data controllers/processors to identify conceivable risk to data and adopt sufficient measures to safeguard data against such risk as equally provided by the Nigerian Regulation. Unlike the Regulation, the aforementioned laws take a step further by requiring data controllers/processors to frequently confirm the effective implementation of these safety measures and ensure the frequent update of such measures in response to new risks or deficiencies in the previous measures. Hence, the parties have a continuing obligation to guarantee the adequacy and efficiency of security measures adopted for the protection of data. The absence of this in the Nigerian Regulation gives the impression that the obligation of a responsible party (data controllers/processors) in Nigeria is a one-off obligation.

The PPIA and GDPA also requires data controllers and processors to notify (as soon as reasonably possible) the applicable regulatory authorities and affected data Subjects of any unauthorized access to and acquisition of personal data. This aims at enabling the data Subject to take proactive protective measures to mitigate the potential consequences of the breach. Due to the fact that the Regulation does not impose a similar obligation on data controllers/processors in Nigeria, disclosure of such a breach lies at their discretion thereby creating room for covering up a breach and delayed disclosure of a breach which in turn delays the execution of proactive mitigation measures by the data Subject.

THE PERSONAL INFORMATION AND DATA PROTECTION BILL IN VIEW OF THE COVID-19 PANDEMIC

The Personal Information and Data Protection bill originated in the House of Representatives in 2015 and was transmitted to the Senate in 2017. It was passed by the National Assembly as a whole in May, 2019 and is yet to be assented to by the President, Muhammadu Buhari.

The bill which is not as extensive as the Regulation does not include the key provisions which are in tandem with international best practices such as the mandatory consent of a data subject to processing, regulation of processing by third parties, appointment of Data Protection Officers by organizations, and as such does not provide measures to prevent against breach of data.

It is pertinent that the Nigerian legislature reconsiders this bill to include provisions which will bring it in line with international best practices. This is even more important in light of the outbreak of the novel COVID-19 Pandemic which requires the Government and

Governmental organizations to "track and trace" affected individuals. Using tools from location tracing to smart phone apps, the Nigerian Government has been able to monitor shifting patterns of movement to decide how best to impose or lift restrictions. A large proportion of the new information being collected by the Government and its organizations fall within the categories of personal data and sensitive personal data.

The outbreak of the Pandemic has also emphasized the importance of backing-up data in order to protect computing assets and avoid the consequence of stolen, lost or failed devices. The NITDA in celebrating World Backup day on the 31st of March, 2020 encouraged all organizations and the general public to make and safely store backup copies of all valuable data, whether from personal computers, servers, storage devices or personal electronic devices such as smartphones and tablets. This is especially in light of the COVID-19 Pandemic and the need for people to work from home as more data is being generated and may not be backed-up appropriately.

In view of the above, an efficient data protection regime is required in Nigeria now more than ever so that the protection of personal data is not sacrificed on the altar of managing the COVID-19 Pandemic.

CONCLUSION

The emergence of the Data Protection Regulation 2019 is a welcome and significant development considering the lack of data protection laws in Nigeria prior to its promulgation. This is acknowledged as a step in the right direction. However, there is potential for the creation of a more robust data protection regime in Nigeria bearing in mind the need to attain international data protection standards.

In this regard, those tasked with the responsibility of law making as well as the administrators of the data protection regime still have their work cut out for them in developing a data protection regime capable of attaining adequate security of data. The Personal Information and Data Protection Bill should be reconsidered by the National Assembly and re-drafted to include provisions which will bring it in line with international best practices. This is particularly important bearing in mind the large amount of personal data presently being processed as a result of the COVID-19 Pandemic. Attention should also be paid to the laws and regulations on Data protection which have been promulgated in other African jurisdictions in order to swiftly develop extensive and efficient data protection laws capable of ensuring adequate safeguard of data.

For more information please contact:

Blackwood & Stone LP

info@blackwoodstone.com

+234 903 3501 613